E-valimised

Tanel Tammet

Sisukord

- Valimiste tüüpe ja protseduure maailmas
- e-valimised ja i-valimised
- Peamised nõuded protseduurile
- Kirja teel hääletamine kui eeskuju eesti e-valimistele
- E-valimiste põhiprotseduur
- E-valimiste viimase aja täiendused
- Töögrupi ideed täiendamiseks ja parandamiseks

Hea teada

- Vana-kreeka keeruline valitsemissüsteem:
- https://en.wikipedia.org/wiki/Athenian_democracy
- Korruptsioon antiik-Rooma valimistel ametlikult keelatud, aga:
- “ … Money was paid for votes; and in order to ensure secrecy and secure the elector, persons called interpretes were employed to make the bargain, sequestres to hold the money until it was to be paid, and divisores to distribute it. ...”

Valimiste kontekste

- Mitte-poliitilised ja poliitilised valimised
- Erakondade nimekirjade ja kandidaatide hääletused
- Riiklikud ja kohalikud valimised
- Referendumid
- ...

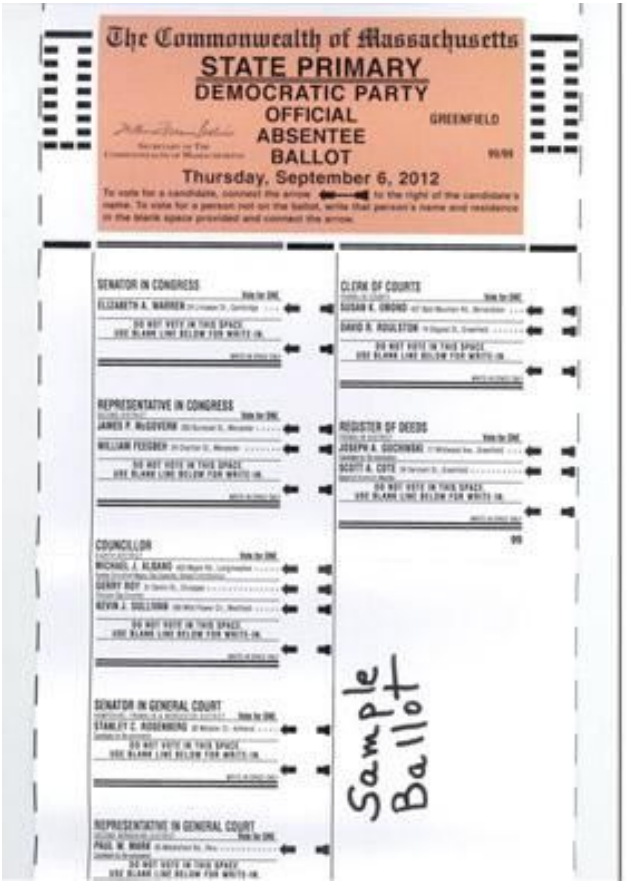
Valimiste tüüpe

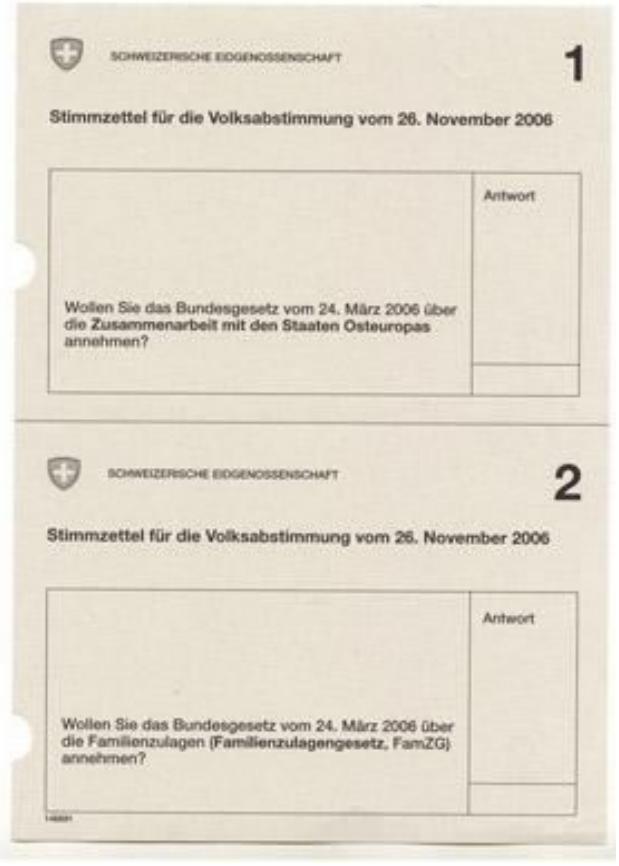
Kuidas otsustatakse võitja(d)?
Vaata https://ncase.me/ballot/

- Majoritaarne: enim hääli saav võidab kõik kohad
- Proportsionaalsed: rohkem hääli saav võidab rohkem kohti
- Järjestatud: saad eelistada/valida mitut

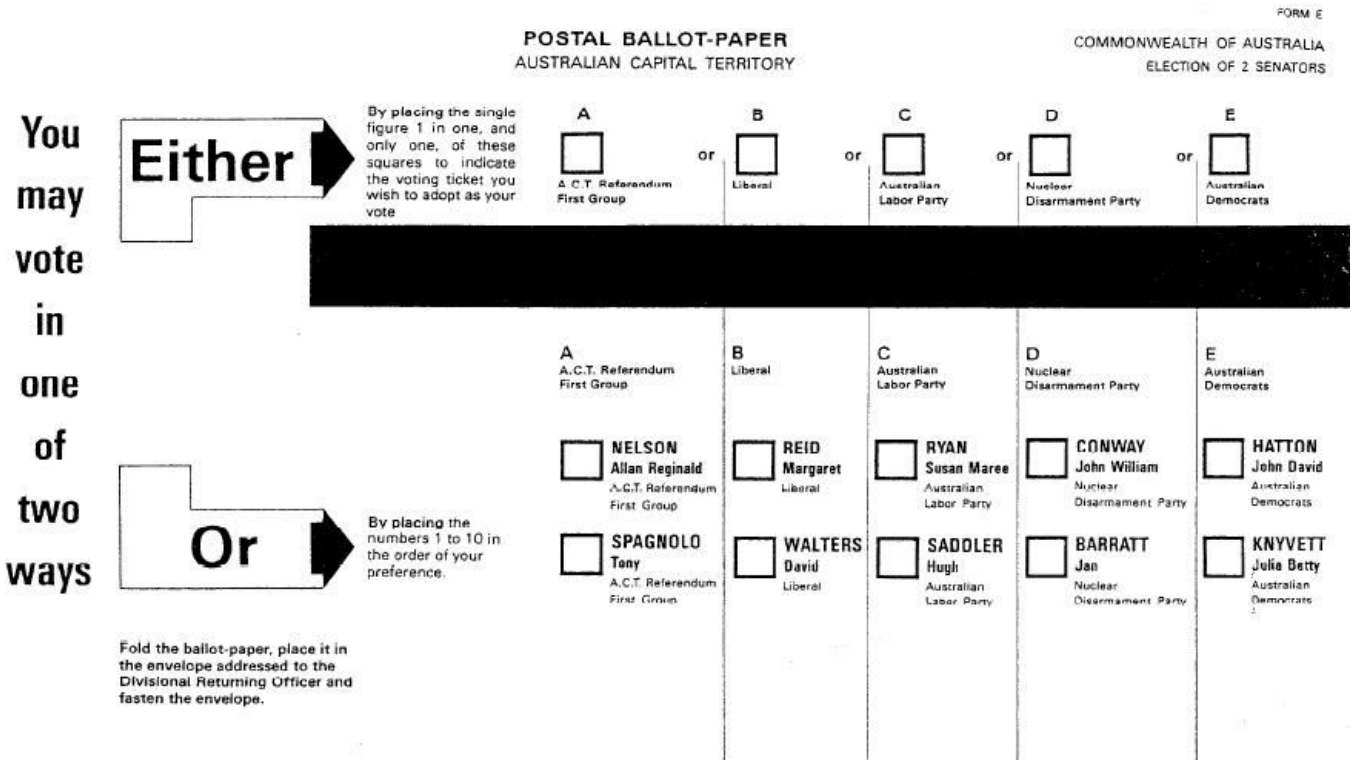
Valimisbülletääne

USA: demokraatide state primary



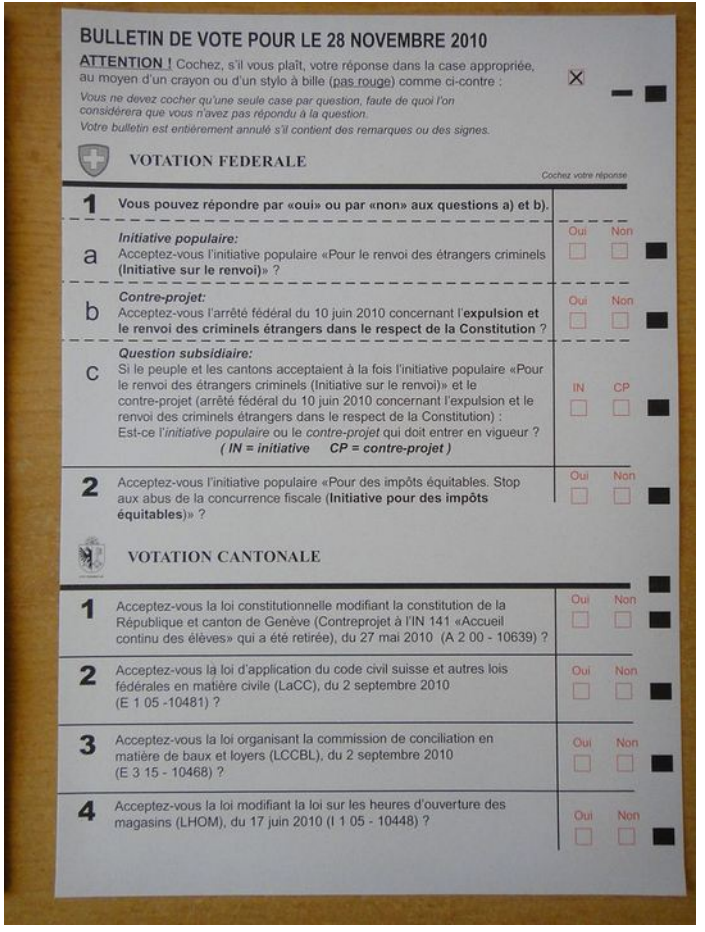


Austraalia kirja teel valimisbülletään

- 

Shveits

- Föderaalne +
- kohalik referendum



BULLETIN DE VOTE POUR LE 28 NOVEMBRE 2010

ATTENTION ! Cochez, s'il vous plaît, votre réponse dans la case appropriée, au moyen d'un crayon ou d'un stylo à bille (pas rouge) comme ci-contre : ☒

Vous ne devez cocher qu'une seule case par question, faute de quoi l'on considérera que vous n'avez pas répondu à la question.
Votre bulletin est entièrement annulé s'il contient des remarques ou des signes.

VOTATION FEDERALE

Cochez votre réponse

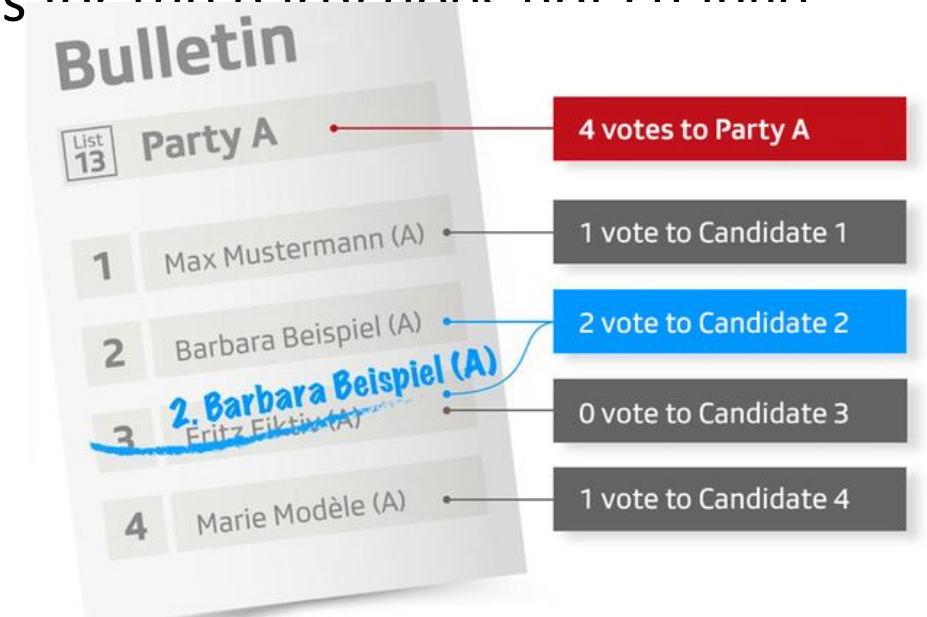
1	**Vous pouvez répondre par «oui» ou par «non» aux questions a) et b).**	
a	***Initiative populaire:*** Acceptez-vous l'initiative populaire «Pour le renvoi des étrangers criminels **(Initiative sur le renvoi)**» ?	Oui ☐ Non ☐
b	***Contre-projet:*** Acceptez-vous l'arrêté fédéral du 10 juin 2010 concernant l'**expulsion et le renvoi des criminels étrangers dans le respect de la Constitution** ?	Oui ☐ Non ☐
c	***Question subsidiaire:*** Si le peuple et les cantons acceptaient à la fois l'initiative populaire «Pour le renvoi des étrangers criminels (Initiative sur le renvoi)» et le contre-projet (arrêté fédéral du 10 juin 2010 concernant l'expulsion et le renvoi des criminels étrangers dans le respect de la Constitution) : Est-ce l'*initiative populaire* ou le *contre-projet* qui doit entrer en vigueur ? ***(IN = initiative CP = contre-projet)***	IN ☐ CP ☐
2	Acceptez-vous l'initiative populaire «Pour des impôts équitables. Stop aux abus de la concurrence fiscale (**Initiative pour des impôts équitables**)» ?	Oui ☐ Non ☐

VOTATION CANTONALE

1	Acceptez-vous la loi constitutionnelle modifiant la constitution de la République et canton de Genève (Contreprojet à l'IN 141 «Accueil continu des élèves» qui a été retirée), du 27 mai 2010 (A 2 00 - 10639) ?	Oui ☐ Non ☐
2	Acceptez-vous la loi d'application du code civil suisse et autres lois fédérales en matière civile (LaCC), du 2 septembre 2010 (E 1 05 -10481) ?	Oui ☐ Non ☐
3	Acceptez-vous la loi organisant la commission de conciliation en matière de baux et loyers (LCCBL), du 2 septembre 2010 (E 3 15 - 10468) ?	Oui ☐ Non ☐
4	Acceptez-vous la loi modifiant la loi sur les heures d'ouverture des magasins (LHOM), du 17 juin 2010 (I 1 05 - 10448) ?	Oui ☐ Non ☐

Valimisbülletääne

Shveits, näiteks: If you want to give additional support to a candidate, you can write their name twice by striking out the name of another candidate of the same party, who lose one vote. However, the total number of votes for the party does not change



Kirja teel valimised maailmas levinud

- Vaata https://en.wikipedia.org/wiki/Postal_voting
- Shveitsis hääletatakse üle 80% kirja teel.
- "In the 2016 US Presidential election, approximately 33 million ballots were cast via mailed out ballots (about 25% of all ballots cast)."
- Rootsis hääletatakse üle 40% kirja teel: väike rootsikeelne ülevaade (kasuta google translate): https://popularhistoria.se/politik/postrostning-demokrati-pa-distans

E-hääletamine ja i-hääletamine

- E-hääletamiseks nimetatakse maailmas tüüpiliselt hääletamismasina kasutamist.
- Interneti teel hääletamine (i-hääletamine) riiklikel valimistel on maailmas väga haruldane.

Mida peab hääletussüsteem tagama?

- Hääled loetakse õieti kokku
- Hääled on anonüümsed
- Ainult hääletamisõiguslikud saavad hääletada, ei saa hääletada topelt, ei saa hääletamist delegeerida
- Häältajaid ei diskrimineerita
- … ja hea oleks häälte ostmist takistada jms ...

E-hääletamine on palju keerulisem, kui internetipangandus

- Internetipanga toimingud ei ole anonüümsed: kõik identifitseeritakse, logitakse ja vajadusel saab minna kohtusse.
- E-hääled on anonüümsed: ei ole võimalik tuvastada, kes kuidas hääletas.

Eesti on ainus!

Eesti on ainuke riik maailmas, mis korraldab üleriiklikke valimisi interneti kaudu.

- Shveits katsetused alates 2001, osades kantonites võimalik, osades ei.
- Kanadas mõned kohalikud omavalitsused.
- Norra KOV 2011 ja piiratult parlament 2013, siis katkestati.

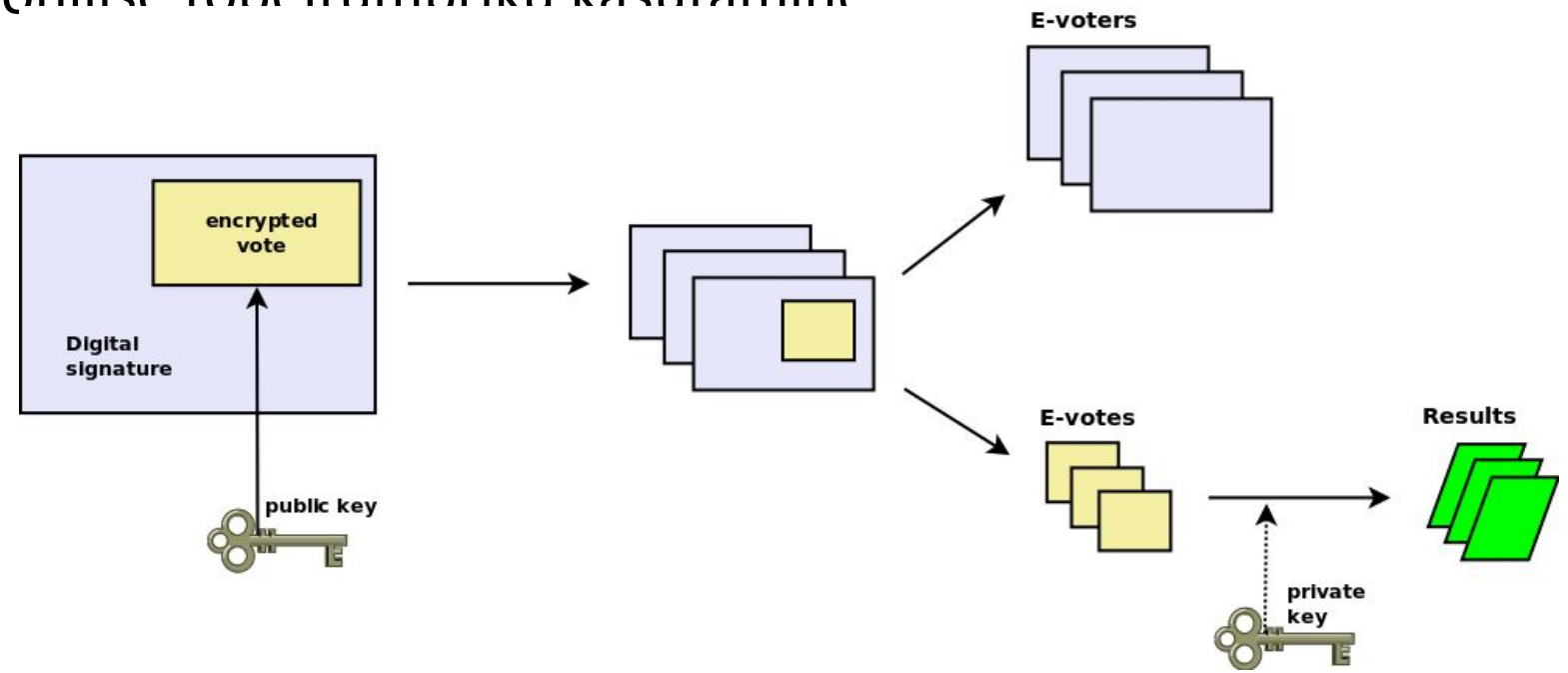
Kirja teel hääletamine

Topeltümbrik:

- Sinu hääl on sisemises ümbrikus: seal ei ole sinu nime
- Sinu nimi on välisel ümbrikul
- Välimise ümbriku järgi sind registreeritakse hääletajaks, võetakse välja sisemine ümbrik ja pannakse valimisurni.

E-hääletamise topeltümbrik

Meie e-valimiste süsteem on algusest peale modelleeritud nimelt posti teel hääletamise elektroonilise variandina. Sellest analoogiast ka elektroonilise topeltümbriku kasutamine



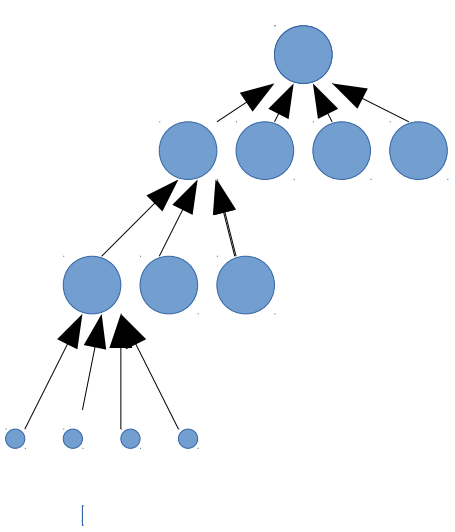
Häälte ostmise raskendamine

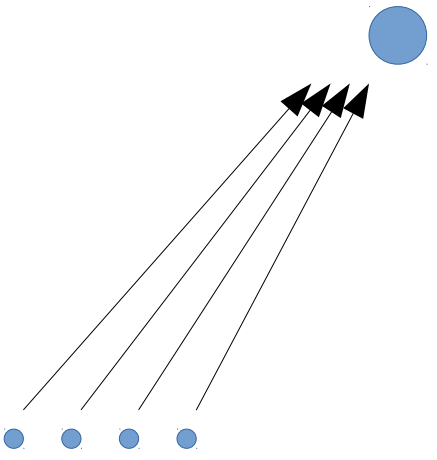
Sama küsimus e-valimistel, nagu kirja teel valimistel: demotiveerida häälte ostmist. Taustaks: häälte ostmine on karistatav. Müümine ei ole karistatav.

- E-häält on lubatud piiramatult muuta ehk üle hääletada
- E-hääle saab muuta valimispäeval jaoskonnas paberil valides

E-valimiste riskide põhiallikas

Tava-valimised: hääli töötleb hajutatult palju inimesi.
E-valimised: häälte töötlemine on tsentraliseeritud.





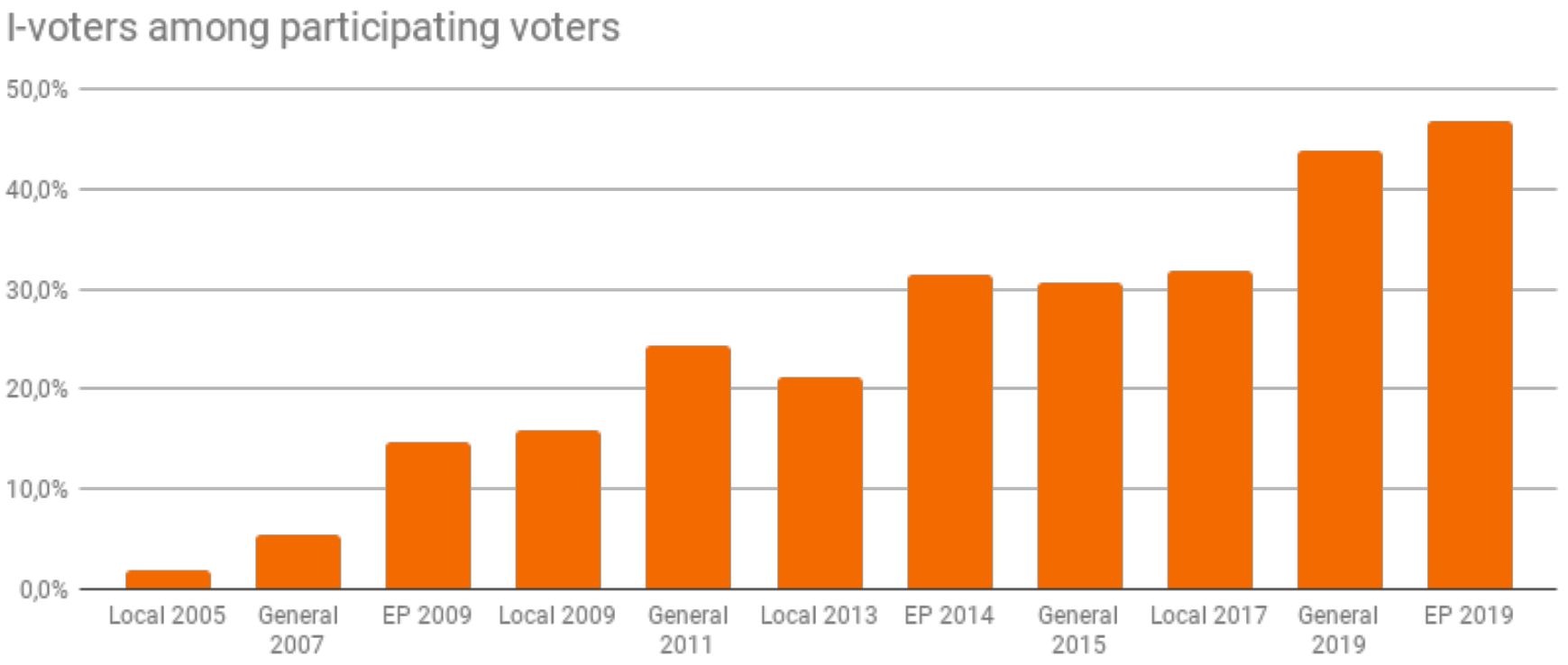
Eesti e-hääletamise materjale

https://www.valimised.ee/et/e-hääletamine/

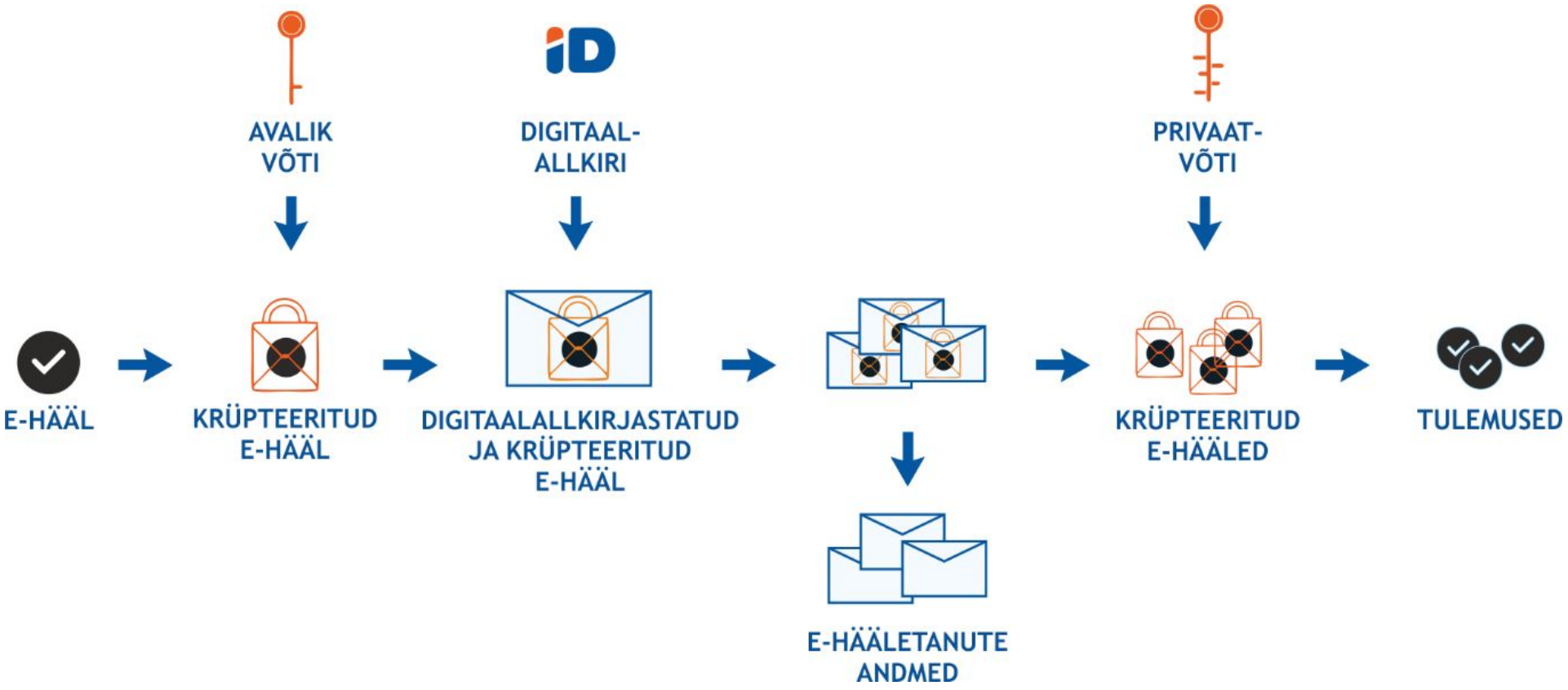
Vt sealt mh:

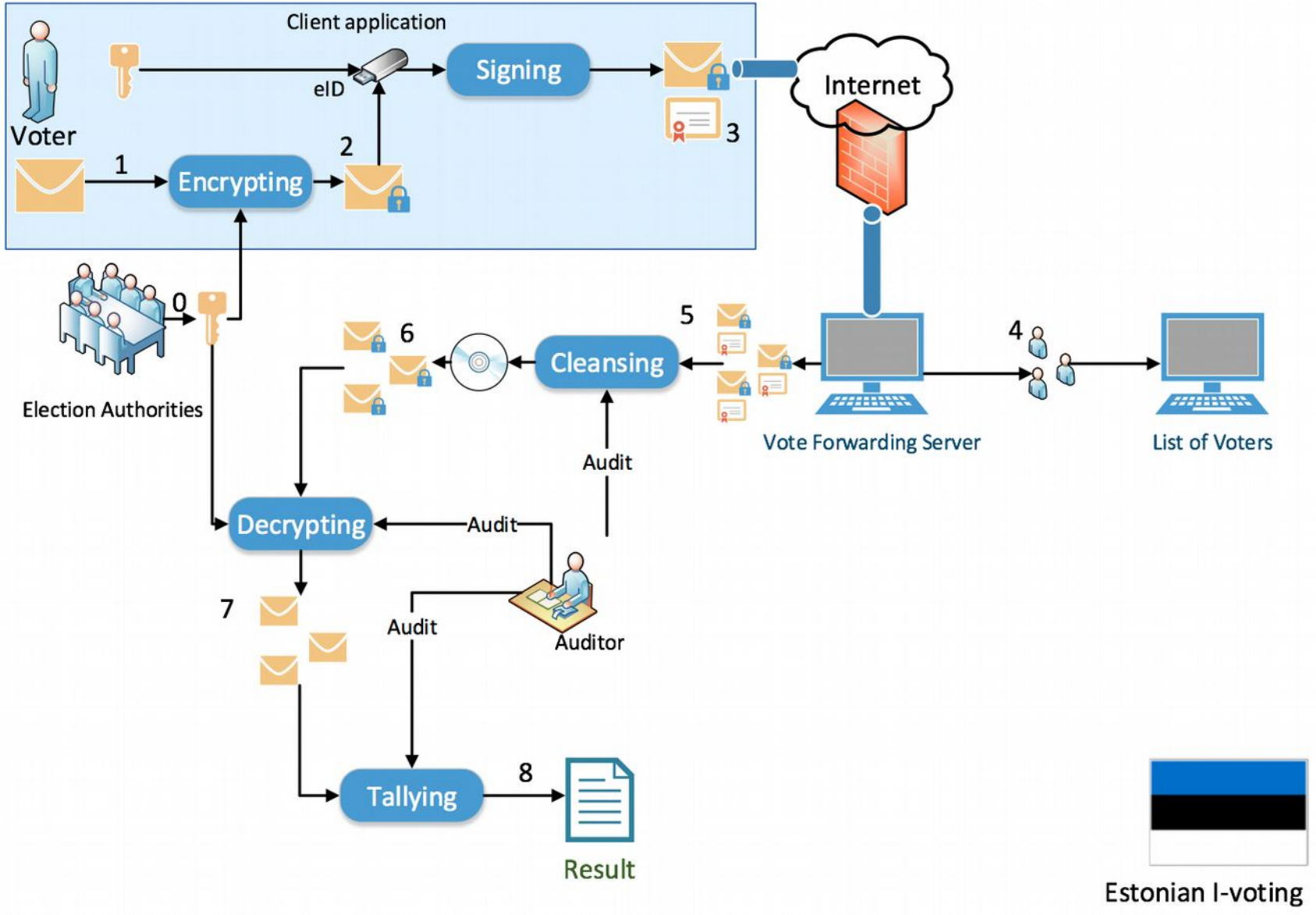
- https://www.valimised.ee/et/e-h%C3%A4%C3%A4letamine/dokumendid
- https://github.com/vvk-ehk/ivxv
- https://www.valimised.ee/sites/default/files/uploads/eh/IVXV_raamistiku_yldkirjeldus_29052017.pdf
- https://www.valimised.ee/sites/default/files/uploads/eh/evalimisteanalyys24okt.doc

E-hääletanute protsent

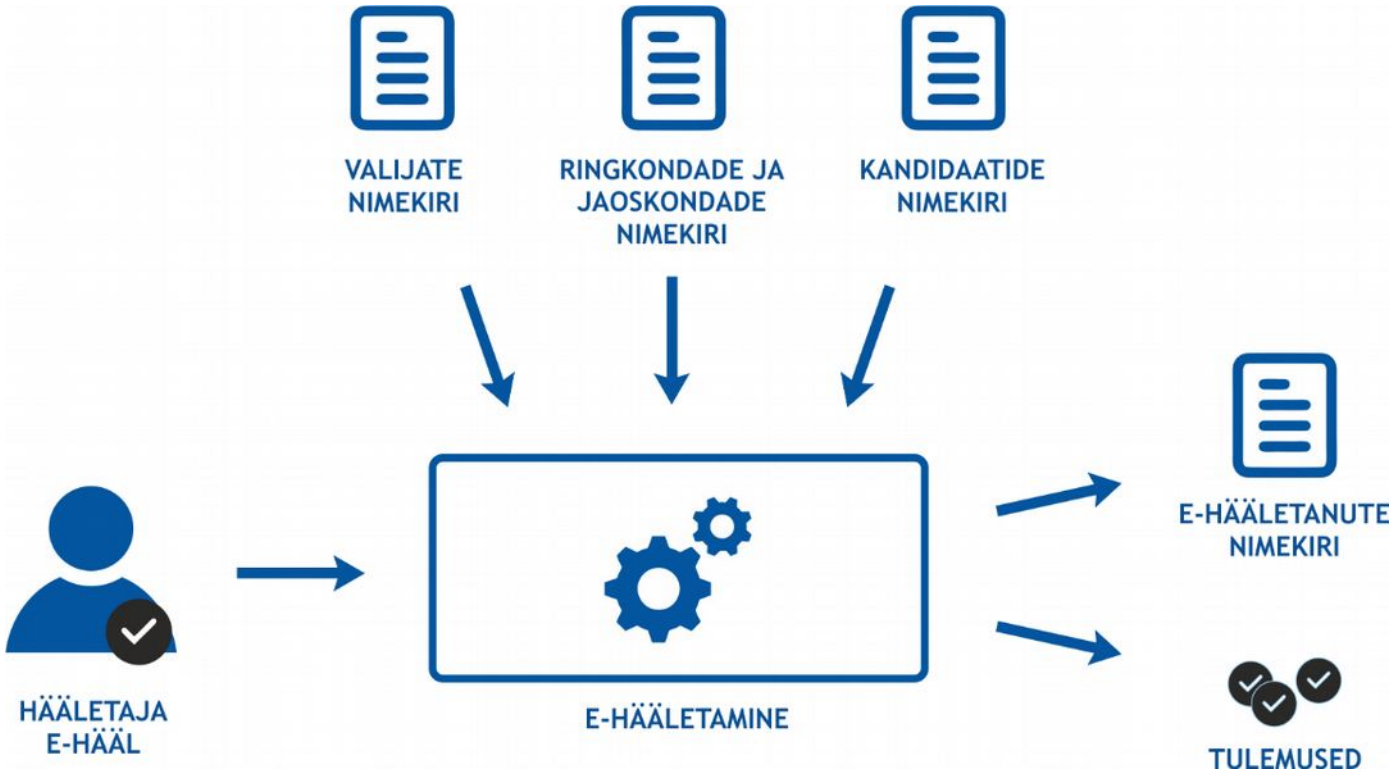


Hääle liikumine süsteemis

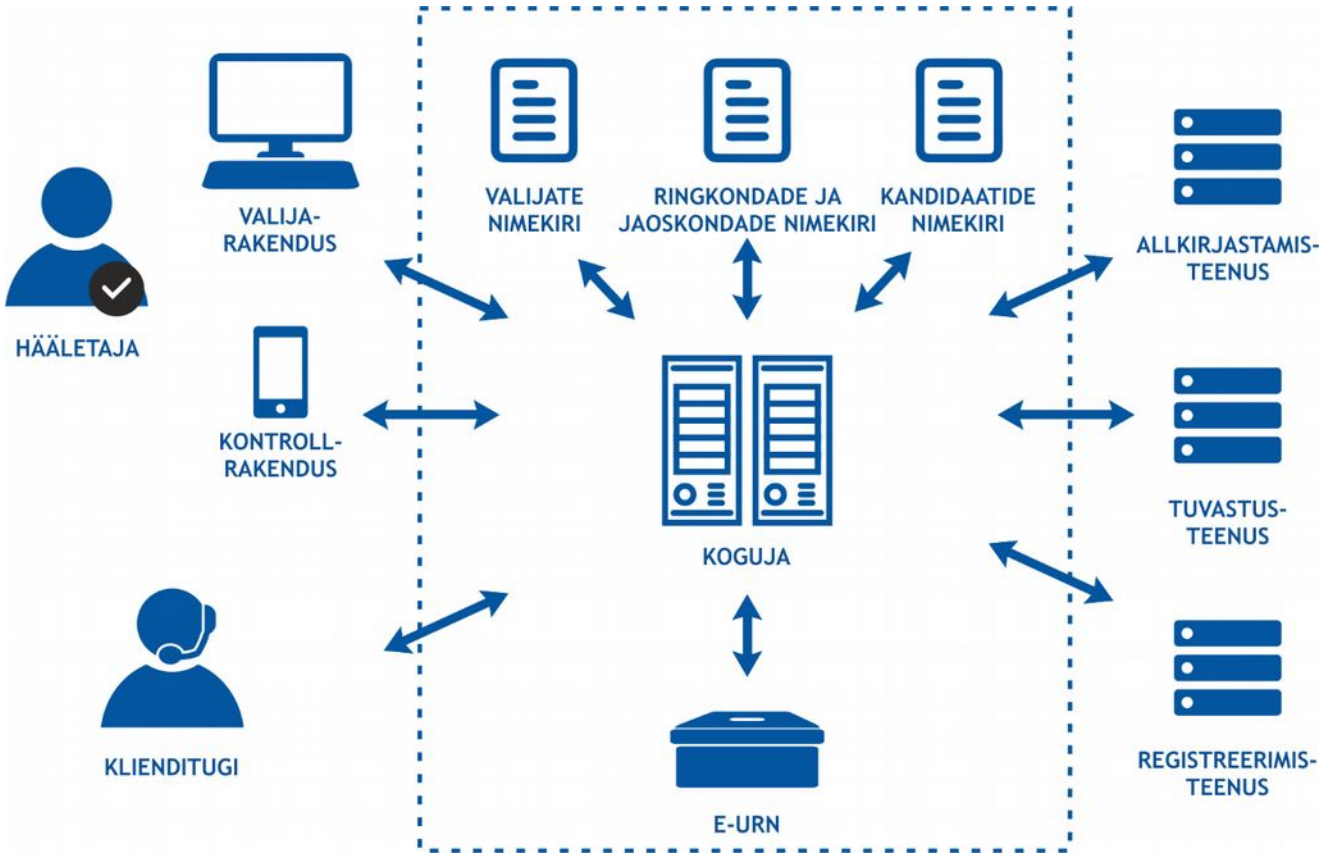



Client application
Voter
eID
Signing
Internet
1
Encrypting
2
3
0
Election Authorities
6
Cleansing
5
Vote Forwarding Server
4
List of Voters
Audit
Decrypting
Audit
7
Audit
Auditor
Tallying
8
Result
Estonian I-voting

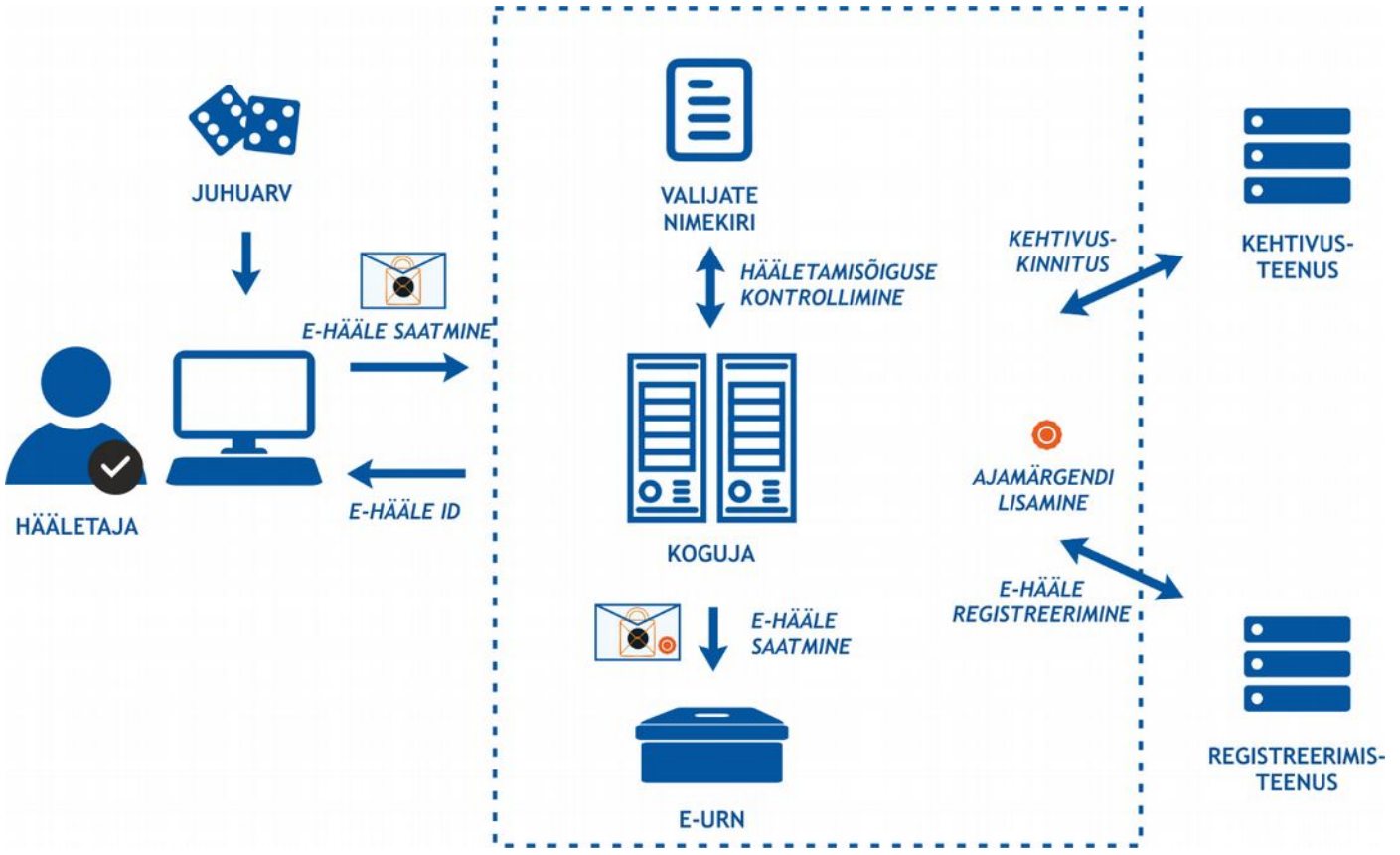
Sisendid ja väljundid



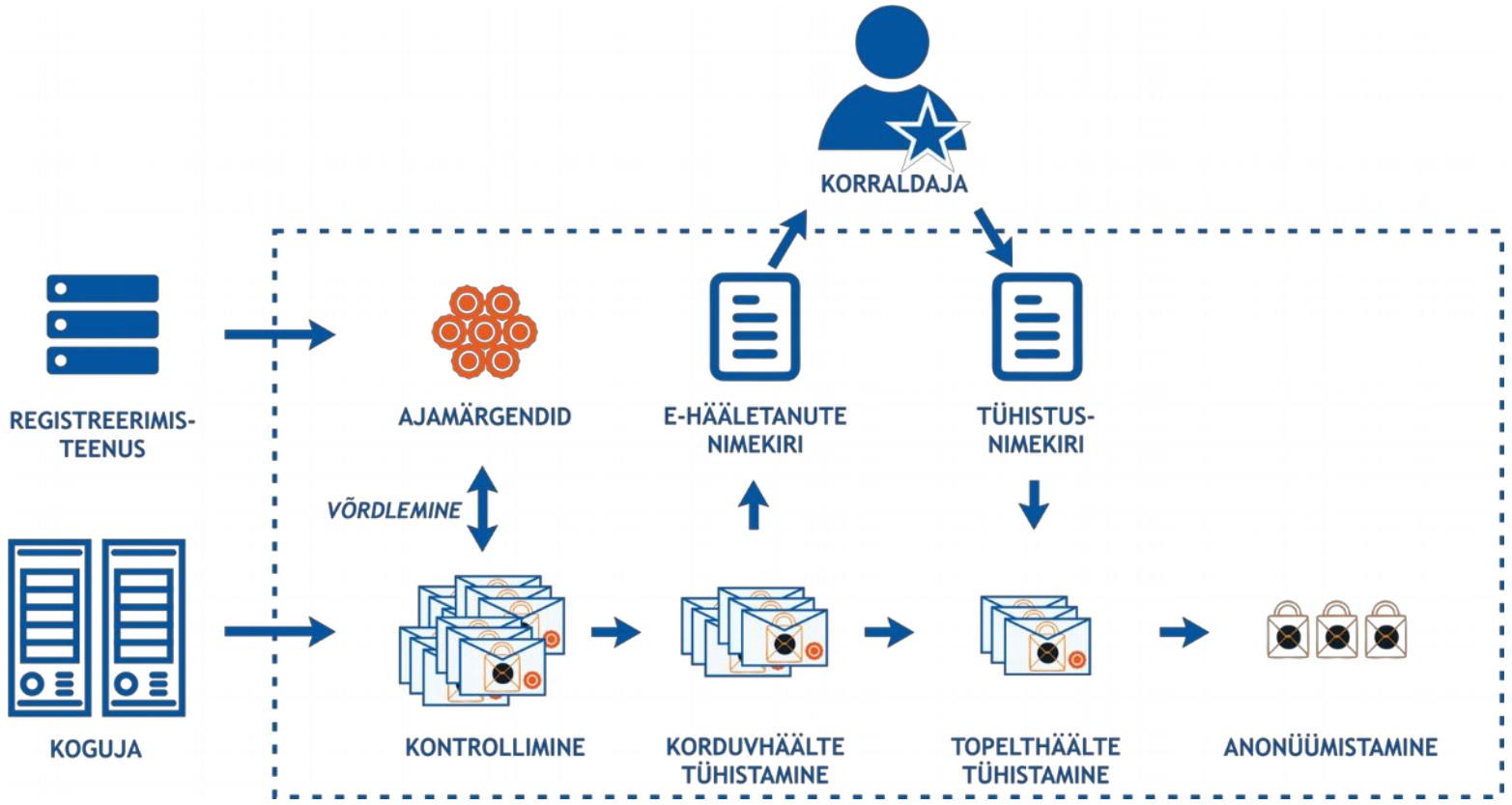
Häälte kogumine



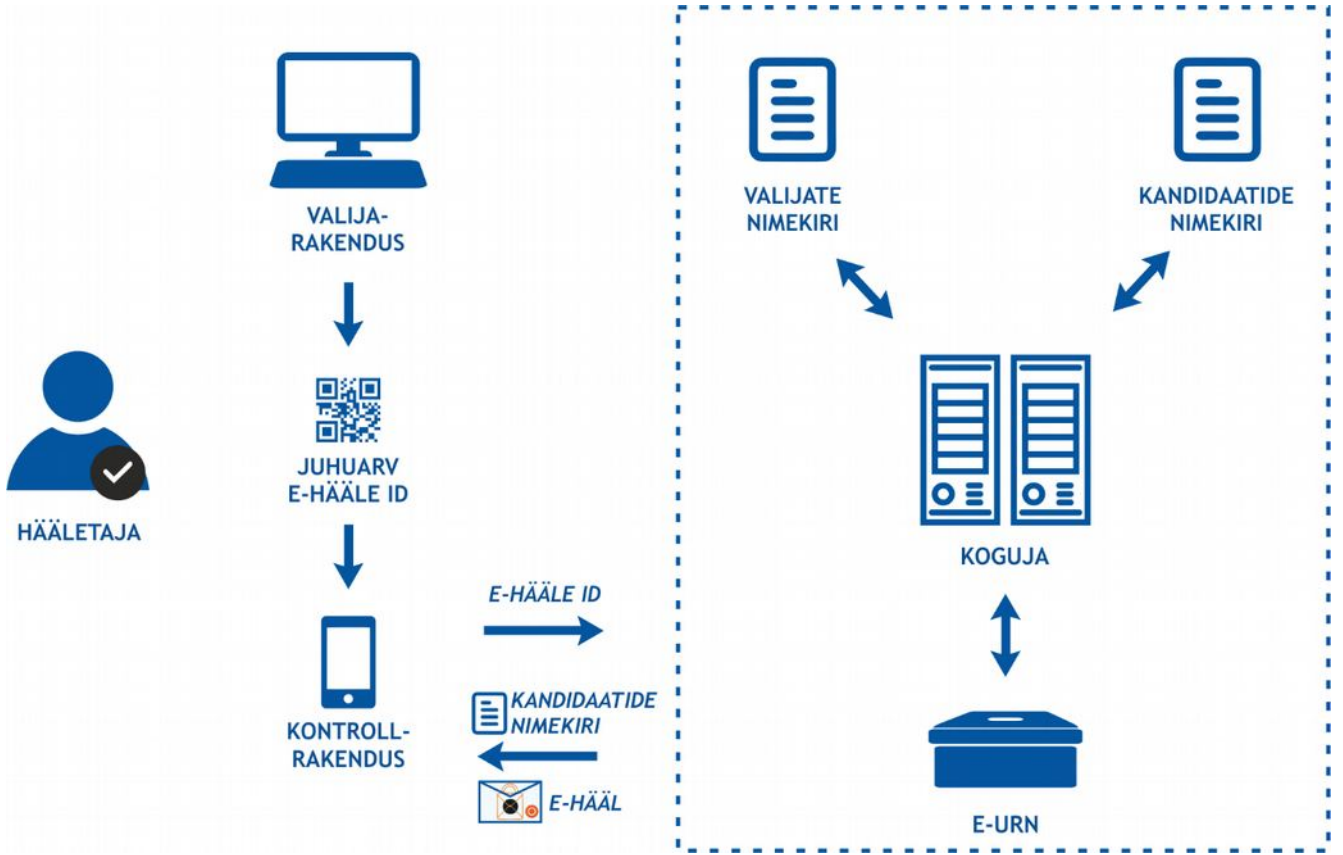
Hääle teele saatmine ja mis siis saab



Hääle töötlemise etapid



Hääle kontrollimisvõimalus mobiilis

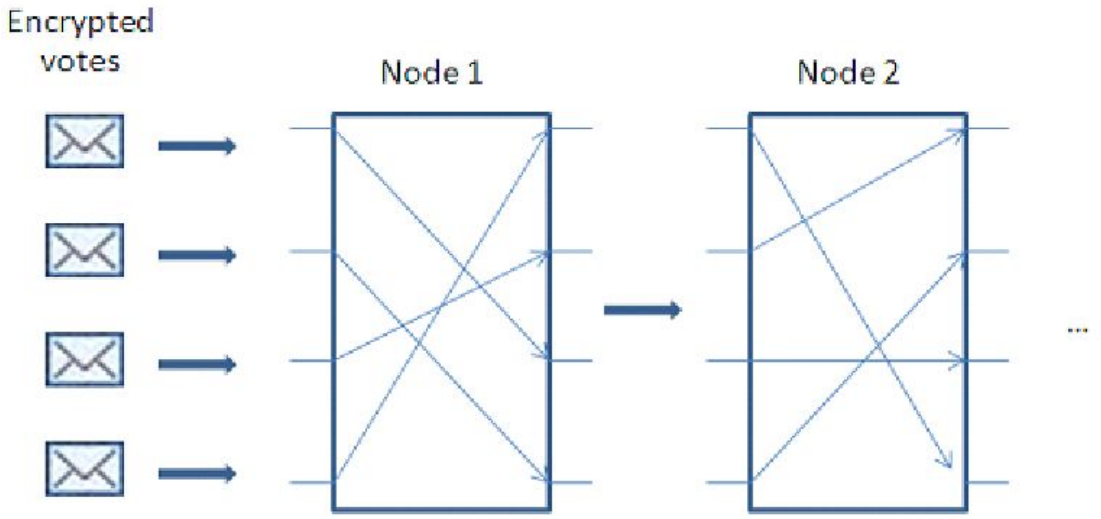


Uued asjad

- Paar korda muutunud: mis perioodil saab e-hääletada
- Vana uus: mobiilist tehtav hääle õige laekumise kontroll.
- Uus uus: mixnet, mis võimaldab häälte kogumise/kokkulugemise kontrolli kindlalt kontrollida.

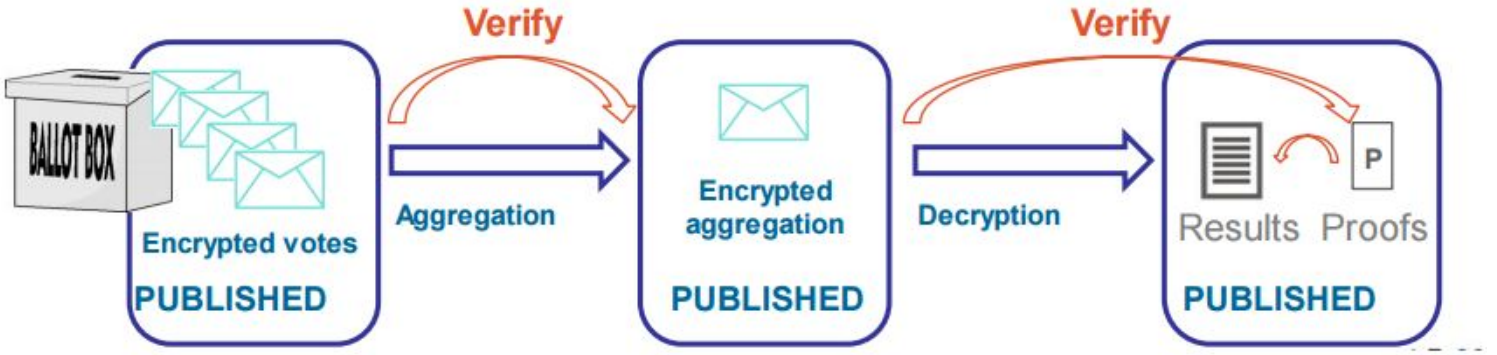
Mixnet

- Eesmärk: segada ära häälte järjekord.
- Eestis kasutatakse: https://www.verificatum.org/



Miksimine alates viimastest valimistest

Enne e-häälte avamist krüpteeritud e-hääled miksitakse, et lugemisele minevaid krüptogramme ei oleks võimalik vastavusse viia valijate e-häältes sisalduvate krüptogrammidega. See võimaldab häälte urni anda auditeerijatele sõltumatuks kontrolliks.



MAJANDUS- JA KOMMUNIKATSIOONI-MINISTEERIUM

E-valimiste töögrupp

Tegevuse ülevaade

8. Oktoober 2019

Eesmärk

Hinnata elektroonilise valimissüsteemi ja elektroonilise hääletamise infosüsteemi protsesside ja turvameetmete **vastavust kehtivatele** küberturvalisust ja valimiste korraldamist käsitlevatele **regulatsioonidele**.

Esimesel koosolekul lepiti kokku (04.07.2019 protokoll):

- et laiemalt **käsitletakse ka muid e-hääletamisega seotud probleeme**;
- **esmajärjekorras keskendutakse siseriiklikule seadusandlusele**.

Rahvusvahelist õigusruumi vaadeldakse juhul, kui Eesti seadusandlus ei vasta rahvusvahelistele tavadele.

Tulem

Töörühm **esitab koondaruande** hiljemalt **12.12.2019**, mis sisaldab hinnangut ja ettepanekuid **süsteemi turvalisuse tagamise** ning **avalikkuse teadlikkuse** tõstmise osas.

Skoop

Töörühm **ei tegele** kõikehõlmava **riskianalüüsi koostamisega**.

Töörühm **käsitleb** ühiskonnas tõstatunud konkreetseid **murekohti**, mis tuuakse ühise arutelulaua taha töörühma liikmete poolt.

Metoodika

1. Etapp Murekohtade kaardistamine.

2. Etapp Murekohtade süstematiseerimine.

3. Etapp Murekohtade sisuline käsitlemine ja lahendusettepanekute tegemine.

4. Etapp Murekohtade hindamine lähtuvalt kehtivatest regulatsioonidest.

5. Etapp Koondraporti koostamine.

Tööplaan

1. **Koosolek** 04. juuli **Eesmärgid ja tööplaan**
2. **Koosolek** 28. august **Murekohtade kaardistus**
3. **Koosolek** 11. september **Murekohtade süstematiseerimine**
4. **Koosolek** september **Murekohtade süstematiseerimine**
5. **Koosolek** oktoober **Lahenduste arutelu**
6. **Koosolek** oktoober **Lahenduste arutelu**
7. **Koosolek** november **Vastavuse hindamine õigusaktidele**
8. **Koosolek** november **Vastavuse hindamine õigusaktidele**
9. **Koosolek** detsember **Koondraporti ülevaatus**

Murekohtade koondtabel

Nr	Murekoht	Kategooria	Prioriteetsus	Keerukus
1.	Süsteemi hoolduse ja arenduse jaoks on liiga vähe ressursse (T. Tammet)	Raha	Kõ3 K M	Ke2 K2
2.	Süsteem ei ole arusaadav vaatlejatele ja avalikkusele (Maaten, T. Tammet)	Teavitus	Kõ K4	Ke K L2
3.	Valikute põhjendamine avalikkusele (Willemson)	Teavitus	Kõ K2 M2	K2 L2
4.	E-hääletamisega seotud valeinfo levitamise minimeerimine (Willemson)	Teavitus	Kõ K M2	Ke3 K
5.	E-hääletamisega on seotud liiga väike grupp inimesi (T. Tammet)	Osalejate hulk	Kõ K4	K4
6.	Sõltumatu kontrolliga tegelevaid audiitoreid on vähe (T. Tammet)	Osalejate hulk	Kõ2 K M2	K L2
7.	Pädevaid vaatlejaid on vähe	Osalejate hulk	Kõ K3 M	Ke2 K2

Murekohtade koondtabel

Nr	Murekoht	Kategooria	Prioriteetsus	Keerukus
13.	Terminid ei ole kooskõlas rahvusvahelise terminoloogiaga (Seeder)	Metoodika	M5	L2
14.	E-hääletamist reguleerivad õigusaktid ei ole selged ja süsteemsed (Seeder)	Õigusaktid	K2 M3	K2
15.	E-hääle liikumine ei ole 100 % vaadeldav (Seeder, Põder)	Protseduurid	Kõ M4	Ke L
16.	E-hääletusel kogutavate isikuandmete formaat on formaliseerimata (Seeder)	Protseduurid	Kõ K M2	L3
17.	Puudub kontroll e-hääletamisega seotud andmete hävitamise üle (Seeder)	Protseduurid	Kõ K M3	Ke L3
18.	E-hääletamise logid ei ole vaatlejale kättesaadavad (Seeder)	Protseduurid	Kõ K M2	K L
19.	E-valimistel puudub hääletuskabiini privaatsus (Seeder)	Protseduurid	Kõ K2 M	Ke L

1.

Murekoht	Selgitus	Võimalik lahendus
Süsteemi jooksva hoolduse ja arenduse jaoks on liiga vähe ressursse (T. Tammet)	Süsteemi jooksev hooldus ja arendus on süsteemi olulisust arvestades liiga vähene. E-hääletuse süsteemile - nii hooldusele, arendusele, läbiviimisele kui kontrollile - kasutatakse liiga vähe ressursse. See takistab otseselt kõigi muude vajalike sammude astumist.	Lahenduseks võiks olla: Viia e-hääletamise tehnoloogiline arendus, hooldus, läbiviimine ja kontroll RIA alla eraldi finantseeritavaks kulukohaks, jättes organisatoorsed, juriidilised jne aspektid Riigikogu Kantseleile. Sõlmida alalised hooldus/arenduslepingud.

2.

Murekoht	Selgitus	Võimalik lahendus
Süsteem ei ole arusaadav vaatlejatele ja avalikkusele (Maaten, T. Tammet)	Fookuses on uued keerulised lisad, mitte põhimõtted ja kontroll. **Süsteemi saidilt on keeruline leida küsimustele vastuseid** (näide: kuidas leida täpseid selgitusi, kes/mis/kuidas sõltumatut kontrolli läbi viivad). Kinnitused, et on olemas videod, ei ole piisav.	Lahenduseks võiks olla uue avalikuks kasutamiseks sobiva **dokumentatsioonisaidi koostamine** (nii eesti kui inglise keeles), mis algab lihtsalt ja põhimõttelistest asjadest ja lingib keerulisi kohti edasi. Võiks kaaluda selle koostamist koostöös ülikoolidega: seal on olemas pedagoogiline kogemus keeruliste asjade lihtsalt ja struktureeritud seletamiseks. Lahendus võiks olla erakondade kaasamine vaatlemisse, nt kohustuslikus

3.

Murekoht	Selgitus	Võimalik lahendus
Valikute põhjendamine avalikkusele (Willemson)	Valimistele esitatavad nõuded on osaliselt vastuolulised - ühest küljest tahame täielikku verifitseeritavust, ideaalis iga ühiskonnaliikme poolt, aga teisalt nõuame valimisvabaduse tagamiseks hääle salajasust. Selliste vastuoluliste nõuete tingimustes tuleb teha kompromisse ja süsteemidisainiotsuseid. Kui pabervalimiste korral on need valikud paika loksunud sajandite jooksul katse-eksituse meetodil, siis elektroonilise hääletamise puhul on palju otsuseid	Ühiskonnas aitaks palju pingeid maha võtta, kui võimalikud valikud ning nende hulgast ühe valimise kriteeriumid ilmutatult kirja saaks, nt raamatus.

4.

Murekoht	Selgitus	Võimalik lahendus
E-hääletamisega seotud valeinfo levitamise tõkestamine (Willemson)	Küsimus on selles, kes, kas ja mida peaks tegema pidevalt e-valimiste ümber levitava valeinfoga. Kas valeinfo levitamist peaks kuidagi sanktsioneerima (ja seda siis kindlasti üldisemalt kui ainult e-valimiste kontekstis)? Kas tõestatult väära info levitamise lõpetamist-ümberlükkamist saab kuidagi nõuda ja jõustada?	

5.

Murekoht	Selgitus	Võimalik lahendus
E-hääletamisega on seotud liiga väike grupp inimesi (T. Tammet)	E-hääletamise avalik usaldusväärsus kannatab, kuna **hääletamise projekteerimise, realisatsiooni ja eeskätt tehnilise läbiviimisega on seotud liiga väike grupp inimesi**. See väiksus tekitab kolm negatiivset efekti: Spetsialistide arv Eestis, kes on hästi tuttavad e-hääletamisega, on väike, seega nemad ja nende tuttavad ei ole väga usaldavad, usaldus ei kiirgu ka laiemale avalikkusele. Uute spetsialistide võimalik hulk, keda saaks kiirelt kaasata, on liiga väike. Väikese hulga läbiviijate puhul on objektiivselt suur risk ni	Lahenduseks võiks olla: 1) Regulaarselt/pidevalt angažeerida suuremat hulka spetsialiste. 2) Suurendada inimeste hulka, kes tegeliku läbiviimise ja kontrolliga tegelevad. Konkreetsem ettepanek selleks: 1) Suurendada e-valimiste pidevat ja igakordset eelarvet 2) Angažeerida projektide kaudu ülikoole nii arendusse kui kontrolli 3) Suurendada läbiviimise ja kontrolli professionaalset meeskonda, duplitseerides ülesandeid eri meeskondade vahel **Siin on käsitluste vastuolu**

6.

Murekoht	Selgitus	Võimalik lahendus
Sõltumatu kontrolliga tegelevaid audiitoreid on vähe (T. Tammet)	E-hääletamise sõltumatu kontrolliga tegelevaid **audiitoreid on vähe** ja nende reaalne **tegevus ja raportid on liiga vähe läbipaistvad**. Samas ei anna ka audiitorite töö parem dokumenteerimine piisavat usaldust. Samuti on **ebapiisav vaatlejate kaasamine**: neil ei ole piisavalt infot ega ligipääsu süsteemi kriitiliste detailide kontrollimiseks. Ainus usaldusväärne viis kriitiliste süsteemide talitluskindluskindluse tõstmiseks on alamsüsteemide duplitseerimine. Süsteem on hetkel küllalt kaoruline ja risk-	Lahenduseks võiks olla: Uues süsteemis võimaliku andmetasemel kontrolli läbiviimine mitme eri meeskonna ja eri tiimi poolt Kogu häälte kogumise ja kokkulugemise süsteemi duplitseerimine eri serverites, eri meeskondade poolt hallatavana ja ideaalis osaliselt erinevate tarkvaradega. Seejuures võiks hääletaja arvutis olev valimistarkvara saata alati hääle kahte kogumisserverisse ja mitte lugeda hääle andmist õnnestunuks, kuni mõlemad ei kinnita vastuvõtmist.

7.

Murekoht	Selgitus	Võimalik lahendus
Pädevaid vaatlejaid on vähe	Vaatlejaid on liiga vähe, kuid valimiste korraldaja ei saa seda otseselt mõjutada. Vaatlejaid mahub füüsiliselt 12 inimest. Suuremat tuba saab kasutada.	Vaatlejate saatmise kohustuslikuks tegemine (erakonnad). Auhind sellele, kes suudab süsteemi sisse häkkida. Koolituse parandamine – selgemaks tegemine. Ekspertide kutsumine valimisi vaatlema. Kaasamine, hallatud diskussioonikeskkond (Chat). IT tudengid võiks saada punkti valimiste vaatlemise ja raporti kirjutamise eest.

8.

Murekoht	Selgitus	Võimalik lahendus
Krüptosüsteemide jätkusuutlikkuse tagamine (Willemson)	Hetkel tuginetakse n-ö klassikalisele asümmeetrilisele krüptograafiale - elliptkõverate või RSA põhine autentimine ja signatuurid, ElGamali krüptosüsteem. Kui kvantarvuti peaks kunagi teoks saama, tuleb nende asemele midagi muud valida. Eriti vajab nuputamist ElGamali krüptosüsteemile asendaja otsimine, sest teadaolevalt pole NIST postkvant-algoritmide kandidaatidelt homomorfsuse omadust nõutud (ja me	1) Post-kvant krüpto uuringute suuna väljaarendamine (KAM uuring). 2) Selgitame, kes selle teemaga saab tegeleda. Üks osa suurest süsteemist.

9.

Murekoht	Selgitus	Võimalik lahendus
Erinevate tehnoloogiate kasutamine häältelugemise protsessis	Mõte tekkis esimesel koosolekul arutelu käigus.	

10.

Murekoht	Selgitus	Võimalik lahendus
Valija arvutis oleva hääletustarkvara kompromiteerimise oht (T. Tammet, Seeder) **Kasutajaliideses välja toomine õige valimiste protsessi ja kinnituse võtmine.**	Valija arvutis oleva hääletustarkvara ründamise/kompromiteerimise korral **võib see anda valehääli või jätta hääled andmata**, ning siis keskse serveri turvamine ei aita. Peame seda muret pigem vähem prioriteetseks, kuna monitooring ja valijapoolne hääle registreerimise kontrollimise võimalus mobiiliga teeb märkamatu mastaapse rünnaku väga keeruliseks ja vähetõenäoliseks. E-hääletajal pole võimalik veenduda, et tema arvuti pole „ära kaaperdatud“ ega suuna teda piraatide	**Kaaluda täpsemalt võimalust kasutada mitut süsteemi.** Võimaliku lahendusena võiks nõuda mobiililt samuti valimist või antud hääle kinnitamist: aktsepteeritakse ainult hääli, kus on hääletatud/kinnitatud nii arvutist kui mobiilist. Arusaadav puudus oleks siin hääletamisprotsessi ebamugavamaks muutmine. Et anda kindlus ühendusest õige serveriga, pannakse valijarakendus e-hääletaja sisenemisel tegema X-tee päringut „isiku dokumendid“ siseneja enda isikukoodiga. E-hääletajale kuvatakse päringu vastus ja ekraanil on kättesaadav nupp kirjaga „Kõik õige. Lähen edasi e-hääletama.“ Vajutades nuppu, alustatakse hääletusprotseduuriga. Peale e-hääletajale kindluse loomist ühendusest õige serveriga ja reaalajas ning end-to-end verifiability kontrollivõimaluste loomist,

11.

Murekoht	Selgitus	Võimalik lahendus
Puudub võimalus mobiiliga hääletada (Seeder) Võimaldada lisaks ID-kaardi ja Mobiil-ID ka Smart-ID-ga e-hääletamine.	Raporti „Digital 2018 Estonia (January 2018)“ andmetel on Eestis 1,84 miljonit kasutuses mobiiliühendust, millest 79% on 3G või 4G. Kuivõrd *broadbandi* (3G ja 4G) saavad kasutada ainult nutitelefonid, siis võime teha järelduse – Eestis on aktiivses kasutuses 1,45 miljonit andmeside funktsionaalsusega SIM-kaarti. Sama raporti andmetel on Eestis 720 000 igakuiselt aktiivset Facebooki kasutajat. Nendest 83% kasutab FB-d nutitelefoni kaudu.	Individuaalse hääletuse kontrollkoodi rakendamisel kaob ära vajadus Kogujast oma e-häält mobiilselt kontrollida. **Mobiiltelefonid vabanevad kasutamiseks e-hääletamise seadmena.** E-hääletamise võimaluse loomine mobiiliga parandab oluliselt võimalusi privaatseks hääletamiseks. Kui arvutid on sageli kas tööandja ruumis või pere ühiskasutuses ruumis, siis mobiil on täpselt seal kus inimene ja ta võib e-hääletamise läbi viia privaatselt.

Murekoht	Selgitus	Võimalik lahendus
Hääletajal puudub võimalus kontrollida hääle jõudmist lugemisele (Seeder)	E-hääletajal on praegu võimalus kontrollida esmast salvestamist ehk „mobiilse kontrolli võimalus“. E-hääletaja ei saa kontrollida, kust süsteem talle kuvatava valiku võtab, lisaks **ei saa kontrollida, kas valik läbib korrektselt ka häälte töötlemise ja lugemise**	**Individuaalse koodi lisamine igale häälele.** **Probleem hääletaja valiku säilitamisega. Vastuolu, sest hääletamise salajasus on olulisem.** **Hääletamise tõendamise küsimus.** **Kas pikendada hääle kontrollimise aega.** **OECD hinnangul seab QR kood ohtu hääletamise salajasuse.** **E-hääle salvestamisele reaalajas kontrollivõimaluse loomine**. Valija võib soovida näha reaalajas „sõltumatust“ allikast, et tema valiku salvestamine Kogujas õnnestub. Sellise võimaluse loomiseks replikeeritakse VVK avalikule veebilehele Koguja logi baasandmed (kellaaeg, IP, hääle salvestamise õnnestumine). Neid peaks saama vaadata ka tagantjärele, mis eeldab kerimisriba või faili salvestamise võimalust. **Lugemisele saabunud e-häälte hulgast oma hääle leidmise võimaluse loomine.** E-hääletajale antakse hääle ärasaatmisel teada tema häälele lisatav unikaalne kontrollkood ning tekib võimalus oma hääl hiljem avalikust häältefailist üles leida ja veenduda, et hääl on kohal ja õigesti kokku loetud. Kontrollkood on individuaalne, see on valimissaladus, ja seda süsteem ega administraator ei saa teada.

13.

Murekoht	Selgitus	Võimalik lahendus
Terminid ei ole kooskõlas rahvusvahelise terminoloogiaga (Seeder)	Praegu Eestis kasutatav terminoloogia tekitab suhtlemisel välismaailmaga segadust, kuna meie e-hääletus tähendab seal i-hääletust (*internet voting*). E-hääletus tähendab välismaailma terminoloogias pabervalimiste tegevuste toetamist elektroonikaga, aga ka elektroonilist hääletust hääletusmasina, telefoni vms vahendusel.	Terminoloogia harmoniseerimine. Kajastatakse soovitustes.

14.

Murekoht	Selgitus	Võimalik lahendus
E-hääletamist reguleerivad õigusaktid ei ole selged ja süsteemsed (Seeder)	Panna õige selgitus	Panna õige selgitus. Õigusslegus peaks tulema uue redaktsiooniga. JUM peab valimisseadust analüüsima. JUM-i töörühm. Tegeleb asjaga.

15.

Murekoht	Selgitus	Võimalik lahendus
E-hääle liikumine ei ole maksimaalselt (100 %) vaadeldav (Seeder, Põder) UUS SÕNASTUS – Anda hääletamise kohta vähem infot, kuid pikema perioodi jooksul. Oma hääle vaadeldavus võiks olla võimalik kuni miksimiseni. Protsessi jälgitavus, mitte üksikhääle jälgitavus. QR koodiga võiks saada	Valimiste usaldusväärsuse tagab selle kõikide protseduuride ja hääle liikumise vaadeldavus. E-häälte töötlemisel on täna mitmeid kohti, kus aga e-hääle liikumise vaadeldavus kaob. Enimtuntud probleemsetest kohtadest on Miksija. Isegi kui õnnestub rakendada käesolevas murekohtade kaardistuses nimetatud individuaalse kontrollkoodi kasutamine, siis ikkagi veel jääb puuduma kontroll näiteks e-häälte ebaseadusliku	Seega on vajalik ka e-häälte töötlemise metoodikat kogu protsessi ulatuses muuta, et võimaldada Miksija jm ohukohtade vahelt ära jätmist ilma mööndustе tegemiseta hääletussaladuse kaitsele. Jaoskonnas üle hääletada, kui on kahtlus e-hääletamise osas.

16.

Murekoht	Selgitus	Võimalik lahendus
E-hääletusel kogutavate isikuandmete formaat on formaliseerimata (Seeder) **UUS: Andmestruktuur peaks olema õigusaktiga kinnitatud.**	Praegu seadus e-hääletuses kogutavate andmete struktuuri ja formaati ei reguleeri. Krüpteeritud ja allkirjastatud e-hääle koosseis on reguleeritud kõige madalamal tasemel – otsusega, mis ei ole õigusakt. Samas on e-hääletuse turvalisuse osas on kriitiliselt oluline, et e-hääles ei sisalduks mitte ühtegi üleliigset tähemärki või vales formaadis tähemärki.	**Andmekoosseisu sätestamine õigusaktiga**. E-häälte salvestamise struktuur ja formaat reguleeritakse seaduses Valimiste üldandmed (mis senise korralduse järgi on iga hääle juures krüpteeringus määratlemata struktuuriga identifikaatorina) pannakse terve faili metaandmestikku ja puudub vajadus nende dubleerimist jätkata iga üksiku hääle metaandmetena). Juhul, kui valimistega samal ajal esitatakse ka mõni rahvahääletuse küsimus, siis küsimus(te)le vastamine tuleks reguleerida eraldi rahvahääletuse seaduse raames (arvestades eeltoodud põhimõtteid). Vastused rahvahääletuse küsimustele allkirjastada, salvestada ja töödelda e-valimiste andmefailist eraldi faili (praegu see põhimõte ei

17.

Murekoht	Selgitus	Võimalik lahendus
Puudub kontroll e-hääletamisega seotud andmete hävitamise üle (Seeder)	E-häälte hävitamine on praegu demonstratiivne ega taga kaitset *insiderite* eest. RKVS § 77’ lg 2 sätestab e-häälte hävitamise 30 päeva peale valimisi, kuid ei sätesta metoodikat, organisatsiooni, vastutust ega anna delegatsiooninormi. E-häälte ja isikuandmete logimise peamise keskuse RIA suhtes puudub väline kontroll e-hääletamisega seotud andmete hävitamise üle. On teadmata, kas ja kui palju RIA sisemised regulatsioonid seda valdkonda	Seadusandlus vajab korrastamist, et välistada e-hääletamise andmestiku koopiate või loetavate fragmentide jäämine RIA-sse, VVK-sse või lekkimine rahvusarhiivist. **Protseduur peab olema kinnitatud / formaliseeritud.**

18.

Murekoht	Selgitus	Võimalik lahendus
E-hääletamise logid ei ole vaatlejale kättesaadavad (Seeder)	Osaledes RK2019 valimistel e-hääletuse vaatlejana, soovisin tutvuda logidega. RIA keeldus põhjendusel, et logid on VVK-le üle antud. VVK keeldus põhjendusel, et logid sisaldavad isikuandmeid.	**Protseduur peab olema reguleeritud, kuidas logid kättesaadavaks teha.** - **Teha ülevaade protsessi käigus tekkinud andmetest.** - **Otsustada, kellele mis andmed kättesaadavaks teha.** E-hääletamise logidega tutvumine peaks olema võimaldatud vähemalt audiitoritele ja vaatlejatele. Muudele isikutele ehk kaasusepõhiselt. See on vajalik elementaarse usalduse (loe: kontrollivõimaluse)

19.

Murekoht	Selgitus	Võimalik lahendus
E-valimistel puudub hääletuskabiini privaatsus (Seeder) **Kuidas olla kindel, et hääletaja on see, kellele on väljastatud ID-kaart.** **Kasutajaliideses välja toomine õige valimiste protsessi ja kinnituse võtmine.**	Kui pabersedeliga hääletamisel kehtib nõue privaatse hääletuskabiini kasutamiseks, siis e-hääletamisel sama nõuet pole. E-hääletada saab praegu ainult arvutitest, kuid **kõigil ei ole privaatse hääletusvõimalusega arvutit.** Privaatse e-hääletusvõimaluse parandamiseks luuakse hääletusvõimalus ka mobiilile ja sätestatakse e-hääletuse privaatsusnõuded rakendusseadustes. Seadus ja jõustruktuurid on vaadanud „läbi sõrmede“ privaatsusnõuete kohaldamisele lähisuhtes isikute vahel või muu	Rakendusseadustes sätestatakse ja avalikkusele kommunikeeritakse, kuidas e-hääletaja ja tema lähikondsed hääletussaladuse kaitse tagavad, nähakse ette (toimivad) sanktsioonid ja jõustruktuuride tegevusplaan rikkumiste minimeerimiseks. Asutustele ja ettevõtetele, millised kasutavad töötajate salajast jälgimist (kaamerad, arvutitöö jälgimine võrgu kaudu), sätestatakse seaduses reeglid jälgimisest teavitamiseks või „jälgimisrahuks“ valimiste perioodil. Mõned on soovitanud ka kehtestada tehnilisi piiranguid, et ühe seadme

20.

Murekoht	Selgitus	Võimalik lahendus
E-hääletamise tõendusmaterjalide säilitamine (Seeder)	E-häälte hävitamine 30 päeva jooksul peale valimisi muudab e-hääle liikumise hilisema rekonstrueerimise võimatuks: Välistab potentsiaalse e-häältega manipuleerija heidutuse valimispettuse jätkuva avastatavuse näol; tekitab e-hääletajate hulgas ebakindlust Kuigi seadus annab õiguse e-hääletamise tulemust veel vaidlustada, siis hääle liikumise läbipaistmatuse ja valimistulemuste töötlemise süsteemi keerukuse tõttu on tulemustes kahtlejal kehtivate reeglite tingimustes peaaegu võimatu hankida lahendi	Kehtestada e-hääletamise tulemusi rekonstrueerida võimaldava andmestiku (e-hääled, e-hääletamise logid) säilitamine üle kahe valimistsükli - 10 aastat alates valimispäevast. Sätestada e-häälte hilisema ülelugemise võimaldamiseks regulatsioon. Jõustada rakendusakt e-häälte rahvusarhiivi üleandmise, säilitamise ja hävitamise korraga. Tulenevalt elektroonilistele valijanimekirjadele üleminekust alates järgmistest valimistest seaduses sätestada valijanimekirjade ja e-hääletamise ajutisele säilitamisele kuuluvate materjalide riigiarhiivile üleandmise elektroonilised formaadid

21.

Murekoht	Selgitus	Võimalik lahendus
E-häälte töötlemisel ei rakendata protokollimist (Seeder)	Protokollimisega kirjeldatakse, kuidas tajuti toimunut reaalajas. Seega on protokollimine vajalik ka siis, kui salvestatakse video. OSCE/ODIHR 2011 aasta raport sedastab, et isegi videole salvestamine ei asenda protokollimist: „Vastavalt VVK juhistele filmiti kõiki protseduure. Kuid on küsitav, kas kõiki tegevusi saab ühe kaameraga dokumenteerida. Igal juhul ei saa selline videosalvestus asendada tavapärast paberkandjal dokumenteerimist.“.	**Protseduuriliselt oleks vaja reguleerida.** Viiakse sisse kõigi olulisemate e-häälte ja logide käitlemise toimingute protokollimine.

22.

Murekoht	Selgitus	Võimalik lahendus
E-hääletus ja paberhääletus on ajaliselt nihkes (Seeder)	E-hääletuse lõppemine ja e-häälte töötlemise algus on ajaliselt nihkes, see loob täiendava riskiteguri ja annab aluse diskussioonile ühetaolisuse põhimõtte tähendusest. Seda on põhjendatud argumendiga, et kui e-hääletamine lõpeb eelhääletamisest 2 tundi varem ega ei toimu valimispäeval, siis saab ebaseadusliku sunni all olnud e-hääletaja minna veel valimisjaoskonda ja muuta oma valiku ära. Paraku on tegemist otsitud argumendiga, sest praktikast ei ole teada ühtegi juhtumit,	**Valimiskomisjon - 2021 olukord muutub.** E-hääletus ja paberhääletus tuleb korraldada paralleelselt, alustades ja lõpetades ühel ajal. Tulemusi tuleb mõlemal juhul hakata lugema koheselt pärast hääletuse lõppemist. Oht, et e-hääletaja hääletamisvabadust rikutakse, tuleb maandada hääletamisvabaduse rikkumisele proportsionaalsete sanktsioonide kehtestamisega, õigusregulatsioonide toimivuse monitoorimise ja jõustruktuuride suunamisega

23.

Murekoht	Selgitus	Võimalik lahendus
E-valimiste tulemuste teatavakstegemise viis ja kiirus võrreldes pabervalimistega (Solvak)	E-valimiste ja pabervalimiste erinevad tulemused tulenevad mittejuhuslikust valijakäitumisest, samas **tekitab inimestes segadust** teatud erakondade suur e-häälte saak võrreldes paberhäältega ja teiste väike e-häälte arv.	**Valimiskomisjon teeb ilusa ja ägeda kodulehe, mis on parem, kui ajakirjanduses.** Üks viis segaduse vähendamiseks on kaaluda hääletustulemuste eri viisidel teatavaks tegemist, näiteks valimisõhtul ringkondade kaupa täielike tulemuste väljatoomine, mitte koheselt valimisviisi kaupa. Tulemusi see ei muuda, aga vähendab ehk esmaseid emotsioone ja juttu et üks või teine erakond "võitis e-valimised".

24.

Murekoht	Selgitus	Võimalik lahendus
E-valimiste usalduse polariseeritus (Solvak)	E-valimised on üldiselt valijate silmis ülimalt kõrge usaldusega, kuid ca 10% valimisõiguslikest ei usalda e-valimisi üldse ning need on kõik paberil valijad. Mõttekoht on seega kas ja kuidas oleks võimalik vähendada usalduse polariseeritust e-valimiste suhtes valijaskonna seas, sest **valimiste korraldusliku poole suhtes võiks ideaalis valitseda konsensus**, vaidlused peaksid olema poliitikate	

MAJANDUS- JA KOMMUNIKATSIOONI-MINISTEERIUM

Aitäh!

Raul Rikk
raul.rikk@mkm.ee